E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 11 No 2 Tahun 2026

EVALUASI MANAJEMEN RISIKO KEAMANAN PADA APLIKASI DANA: ANALISIS BERBASIS FREKUENSI, DAMPAK, DAN TATA KELOLA IT

Achmad Ersyad1, Eka Sastra Bomin2, Adnan Afief Zain3
[1,2,3] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muslim Indonesia, Makassar (Email: 13020230312@student.umi.ac.id, 13020230295@student.umi.ac.id, 13020230066@student.umi.ac.id)

ABSTRACT

This study aims to evaluate security risk management in the DANA application using a frequency and impact-based approach within the IT governance framework. The method employs quantitative risk matrix analysis based on ISO 31000:2018 and COBIT 2019 standards, drawing on secondary data from national news media, public incident reports, OJK/BI regulations, and academic literature. Eight primary risks were identified, with social engineering and phishing attacks receiving the highest risk score of 20 (High category), followed by account compromise via malware and fake APK with a score of 16 (High category). The remaining six risks fell into the Medium category with scores of 5-9. Recommended mitigation strategies include strengthening AI-based in-app security features, server autoscaling automation, periodic penetration testing, and least privilege access control. This study confirms that user psychological manipulation-based threats represent the top priority in the IT governance of digital financial applications in Indonesia.

Keywords: risk management; information security; DANA application; IT governance; ISO 31000.

ABSTRAK

Penelitian ini bertujuan mengevaluasi manajemen risiko keamanan pada aplikasi DANA menggunakan pendekatan berbasis frekuensi dan dampak dalam kerangka tata kelola teknologi informasi. Metode yang digunakan adalah analisis kuantitatif dengan matriks risiko mengacu pada standar ISO 31000:2018 dan COBIT 2019, dengan sumber data sekunder dari media massa nasional, laporan insiden publik, regulasi OJK/BI, dan literatur akademis. Delapan risiko utama berhasil diidentifikasi, di mana serangan social engineering dan phishing memperoleh skor risiko tertinggi sebesar 20 (kategori Tinggi), diikuti penyalahgunaan akun via malware dan APK palsu dengan skor 16 (kategori Tinggi). Enam risiko lainnya berada pada kategori Sedang dengan skor 5-9. Strategi mitigasi yang direkomendasikan mencakup penguatan fitur keamanan in-app berbasis AI, otomatisasi autoscaling server, penetration testing berkala, serta pembatasan hak akses berbasis prinsip least privilege. Penelitian ini menegaskan bahwa ancaman berbasis manipulasi psikologis pengguna merupakan prioritas utama dalam tata kelola IT aplikasi keuangan digital di Indonesia.

Kata Kunci: manajemen risiko; keamanan informasi; aplikasi DANA; tata kelola IT; ISO 31000.

Article History
Received :Juli 2026
Reviewed:Juli 2026
Published: Juli 2026

Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi besar dalam sektor keuangan, khususnya melalui kemunculan layanan keuangan digital atau financial technology (fintech). Di Indonesia, berkembang ekosistem sangat pesat fintech seiring meningkatnya penetrasi internet dan penggunaan telepon pintar. Salah satu pemain utama di industri ini adalah DANA, sebuah platform layanan keuangan digital berbasis aplikasi (ewallet dan digital wallet) yang dirancang untuk memudahkan transaksi non-tunai secara online maupun offline dengan cepat, praktis, dan aman (Al Qorny, 2023; Galang & Ramdhan, 2023). Secara legalitas, platform DANA dikembangkan dan dikelola oleh PT Espay Debit Indonesia Koe yang resmi didirikan pada tahun 2017 dan mulai beroperasi penuh melayani masyarakat Indonesia sejak tahun 2018. Sebagai penyedia jasa pembayaran digital, PT Espay Debit Indonesia Koe telah memperoleh izin resmi dari Bank Indonesia (BI) sebagai penyedia e-money, dompet elektronik, layanan kirim uang, dan likuiditas digital. DANA didirikan dengan visi menjadi jembatan menuju masyarakat Indonesia yang bebas tunai (cashless society) sekaligus mendorong inklusi keuangan nasional, terutama bagi masyarakat yang belum terjangkau layanan perbankan konvensional atau unbanked (Salsabila et al., 2023; Umiyati et al., 2021). Sebagai salah satu market leader di industri fintech Indonesia, PT Espay Debit Indonesia Koe menempatkan aspek keamanan data dan transaksi sebagai fondasi utama operasionalnya. Platform ini didukung infrastruktur teknologi kelas dunia dengan sertifikasi keamanan internasional seperti PCI-DSS (Payment Card Industry Data Security Standard) dan ISO/IEC 27001 untuk sistem manajemen keamanan informasi. Komitmen tersebut diwujudkan melalui implementasi fitur DANA Protection, sebuah sistem jaminan keamanan berlapis yang menggunakan teknologi Risk Engine, pemindaian biometrik, serta jaminan garansi uang kembali jika terjadi kegagalan sistem atau fraud yang memenuhi syarat validasi perusahaan (Utomo & Rahman, 2024; Syadzwah et al., 2024). Meskipun demikian, berkembangnya ekosistem digital membawa serta peningkatan ancaman siber yang semakin kompleks. Risiko pada aplikasi keuangan digital tidak hanya bersumber dari celah teknis infrastruktur seperti kerentanan API, kegagalan sinkronisasi saldo, atau gangguan operasional server, tetapi juga dari faktor kelengahan pengguna (human error) yang dieksploitasi melalui berbagai modus penipuan berbasis rekayasa sosial. Penelitian Prastiwi et al. (2024) menegaskan bahwa ancaman terhadap keamanan data pribadi pada aplikasi mobile keuangan semakin beragam dan memerlukan respons tata kelola yang sistematis. Senada dengan hal tersebut, Nurrahma et al. (2025) menemukan bahwa persepsi konsumen terhadap keamanan data masih menjadi faktor kritis yang mempengaruhi kepercayaan dan loyalitas pengguna e-wallet. Uskono et al. (2025) dalam studi komparatif keamanan aplikasi fintech di Indonesia yang melibatkan OVO, GoPay, ShopeePay, dan DANA, menemukan bahwa masing-masing platform memiliki profil risiko yang berbeda-beda, namun secara umum ancaman terbesar tetap bersumber dari serangan berbasis rekayasa sosial dan lemahnya kesadaran keamanan pengguna. Selain itu, Tarigan (2025) menganalisis pola tren transaksi mencurigakan

pada aplikasi DANA selama periode 2020-2024 dan menemukan peningkatan signifikan dalam upaya fraud digital dari tahun ke tahun, yang mengindikasikan perlunya sistem deteksi anomali yang lebih canggih. Berdasarkan latar belakang tersebut, evaluasi manajemen terstruktur risiko menggunakan secara standar internasional menjadi suatu keharusan guna memastikan kelangsungan layanan dan kepercayaan publik. Penelitian ini bertujuan untuk: (1) mengidentifikasi potensi risiko keamanan pada ekosistem aplikasi DANA, (2) menganalisis tingkat frekuensi dan dampak dari masing-masing risiko, (3) mengevaluasi prioritas risiko menggunakan matriks ISO 31000, dan (4) merumuskan rekomendasi strategi perlakuan risiko dalam perspektif tata kelola IT berbasis COBIT 2019.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan metode analisis risiko berbasis matriks. Objek penelitian adalah ekosistem aplikasi DANA yang dikelola oleh PT Espay Debit Indonesia Koe sebagai salah satu platform dompet digital terbesar di Indonesia. Model penelitian diadaptasi dari siklus manajemen risiko ISO 31000:2018 yang dikombinasikan dengan perspektif tata kelola IT dari COBIT 2019, mencakup enam tahapan utama: Komunikasi dan Konsultasi, Penetapan Identifikasi Risiko, Analisis Konteks, Risiko, Evaluasi Risiko, dan Perlakuan Risiko (Syadzwah et al., 2024).

2.1 Sumber Data

Data yang digunakan merupakan data sekunder yang diperoleh dari beberapa sumber, yaitu: (1) laporan insiden dan berita dari media massa nasional terpercaya (Kompas.com, Detikcom) terkait kasus penipuan, gangguan layanan, dan penyalahgunaan aplikasi DANA; (2) laporan pengaduan publik dari platform Media Konsumen yang mendokumentasikan keluhan pengguna secara real-time; (3) publikasi edukasi dan FAQ resmi platform DANA terkait fitur keamanan dan prosedur penanganan insiden; (4) regulasi dan peraturan resmi dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) terkait perlindungan data dan standar keamanan fintech; serta (5) literatur akademis dari Google Scholar yang diterbitkan dalam rentang 2021-2026 yang membahas manajemen risiko keamanan informasi dan keamanan aplikasi fintech (Prastiwi et al., 2024; Uskono et al., 2025).

2.2 Teknik Penilaian Risiko

Penilaian risiko dilakukan menggunakan dua variabel utama. Pertama, Analisis Frekuensi (Likelihood Analysis) yang mengukur seberapa sering suatu insiden keamanan siber atau kegagalan sistem terjadi pada aplikasi DANA dalam periode tertentu, dengan skala 1 (Sangat Jarang/Rare: insiden hampir tidak pernah terjadi) hingga 5 (Hampir Pasti/Almost Certain: insiden terjadi setiap hari). Kedua, Analisis Dampak (Impact Analysis) yang mengukur tingkat kerugian jika insiden tersebut benar-benar terjadi, ditinjau dari tiga aspek yaitu dampak finansial, dampak operasional, dan dampak reputasi, dengan skala 1

(Sangat Rendah: tidak ada kerugian finansial dan gangguan minor) hingga 5 (Sangat Tinggi: pembobolan basis data utama, sistem mati total, dan sanksi hukum dari regulator). Tingkat risiko dihitung menggunakan formula: Risk Level = Frequency x Impact. Hasil perkalian kemudian dipetakan ke dalam Matriks Risiko 5x5 dengan kategori: Rendah (skor 1-4), Sedang (skor 5-9), Tinggi (skor 10-15), dan Sangat Tinggi (skor 16-25) (Rofi, 2022; Savitri, 2021).

2.3 Formula Evaluasi Risiko

Tingkat risiko dihitung menggunakan formula matriks risiko standar.

$$\textit{Risk Level} = \textit{Frequency (F)} \times \textit{Impact (D)}$$

Hasil perkalian kemudian dipetakan ke dalam matriks risiko: Rendah (1–4), Sedang (5–12), Tinggi (13–25). Standar acuan model mengadopsi ISO 31000:2018 sebagai panduan arsitektur siklus risiko dan COBIT 2019 domain APO12 (Managed Risk) serta EDM03 (Ensured Risk Optimization) sebagai perspektif Tata Kelola IT

3. HASIL DAN PEMBAHASAN

Berdasarkan analisis historis gangguan layanan, laporan keluhan pengguna di media massa, dan modus penipuan siber yang marak di industri fintech, delapan potensi risiko utama berhasil dipetakan pada ekosistem aplikasi DANA

Tabel 1 : Hasil Penilaian dan Dampak Risiko Aplikasi DANA

No	Kemungkinan Risiko (Insiden)	Frekuensi (F)	Dampak (D)
1	Serangan Social Engineering & Phishing (Penipuan OTP/PIN)	5	4
2	Penyalahgunaan Akun via Malware/APK Palsu	4	4
3	Kegagalan Sistem Pembayaran (Downtime Server)	3	3
4	Gagal Sinkronisasi Saldo (Delay Topup)	4	2
5	Eksploitasi Celah Keamanan (Vulnerability API)	1	5
6	Penyalahgunaan Fitur Paylater/Limit Kredit	3	3
7	Kegagalan Verifikasi KYC Akun Premium	3	2
8	Kebocoran Data oleh Pihak Dalam (Insider Threat)	1	5

3.1 Evaluasi Risiko dan Matriks Prioritas

Evaluasi risiko dilakukan dengan mengalikan nilai Frekuensi (F) dan Dampak (D) setiap risiko untuk menghasilkan Risk Score. Hasil perkalian kemudian dipetakan ke dalam matriks risiko standar ISO 31000

guna menentukan kategori dan prioritas penanganan. Berdasarkan hasil evaluasi pada Tabel 2, dari delapan risiko yang dianalisis, terdapat 2 risiko dalam Kategori Tinggi (High Risk) dengan skor 16-20, dan 6 risiko dalam Kategori Sedang (Medium Risk) dengan skor 5-9. Tidak ditemukan risiko dalam kategori Sangat Tinggi (Very High) yang mengindikasikan bahwa sistem kontrol keamanan dasar DANA telah berfungsi cukup baik dalam menekan frekuensi insiden katastrofis (Putri et al., 2021; Syadzwah et al., 2024).

Tabel 2. Matriks Evaluasi Tingkat Risiko Aplikasi DANA

No	Kemungkinan Risiko	F	D	Skor	Kategori
1	Social Engineering & Phishing	5	4	20	Tinggi
2	Malware/APK Palsu	4	4	16	Tinggi
3	Downtime Server	3	3	9	Sedang
4	Delay Top-up	4	2	8	Sedang
5	Vulnerability API	1	5	5	Sedang
6	Paylater/Limit Kredit	3	3	9	Sedang
7	Kegagalan KYC	3	2	6	Sedang
8	Insider Threat	1	5	5	Sedang

Serangan Social Engineering dan Phishing menempati urutan tertinggi dengan skor risiko 20 karena modus ini hampir pasti terjadi setiap hari menargetkan kelengahan pengguna. Hal ini sejalan dengan temuan Tarigan (2025) yang mengidentifikasi peningkatan signifikan pola transaksi mencurigakan berbasis rekayasa sosial pada aplikasi DANA selama 2020-2024. Penyalahgunaan akun via malware/APK palsu menyusul dengan skor 16 karena meski tidak terjadi setiap hari, dampak kehilangan kendali akun bersifat sangat merugikan pengguna secara finansial (Utomo & Rahman, 2024). Sementara risiko teknis seperti Vulnerability API dan Insider Threat memiliki frekuensi sangat rendah (skor 1) namun dampak fatal (skor 5), sehingga keduanya tetap menuntut perhatian serius meski berada pada kategori Sedang. Kondisi ini selaras dengan penelitian Uskono et al. (2025) yang menemukan bahwa risiko teknis pada platform fintech Indonesia umumnya rendah frekuensinya namun berpotensi katastrofis bila terjadi. Perlakuan Risiko (Risk Treatment) Berdasarkan prinsip Tata Kelola IT dan framework ISO 31000, usulan perlakuan risiko diprioritaskan mulai dari risiko dengan level tertinggi guna memastikan alokasi sumber daya keamanan siber pada aplikasi DANA berjalan secara efisien dan tepat sasaran (Rofi, 2022; Syadzwah et al., 2024). Mayoritas risiko mendapatkan opsi Mitigasi (Risk Reduction) sebagai strategi penanganan utama. Untuk risiko pertama yaitu Serangan Social Engineering dan Phishing (Skor 20), strategi yang direkomendasikan adalah mengoptimalkan fitur edukasi keamanan terintegrasi pada aplikasi dalam bentuk pop-up warning

wajib setiap kali pengguna akan memasukkan kode OTP atau mengakses fitur sensitif, memperketat deteksi Risk Engine terhadap aktivitas login dari perangkat mencurigakan, serta memperluas kampanye anti-phishing di media sosial resmi DANA. Rekomendasi ini diperkuat oleh temuan Utomo dan Rahman (2024) yang menegaskan bahwa edukasi aktif berbasis aplikasi terbukti meningkatkan kesadaran keamanan pengguna e-wallet secara signifikan. Untuk risiko kedua yaitu Malware dan APK Palsu (Skor 16), strategi yang direkomendasikan adalah Mitigasi dan kombinasi Pengalihan, mengimplementasikan fitur yakni DANA Protection yang menjamin pengembalian saldo untuk kasus fraud yang tervalidasi, serta meningkatkan kemampuan proteksi in-app agar aplikasi otomatis memutus sesi apabila mendeteksi adanya overlay software berbahaya di perangkat pengguna. Selain itu, perlu dilakukan kerja sama aktif dengan platform distribusi aplikasi (Google Play Store dan App Store) untuk segera melaporkan dan menghapus APK palsu yang mengatasnamakan DANA (Prastiwi et al., 2024). Untuk risiko ketiga yaitu Downtime Server (Skor 9) dan risiko keempat yaitu Delay Top-up (Skor 8), strategi mitigasi mencakup otomatisasi autoscaling pada infrastruktur cloud server untuk mengakomodasi lonjakan trafik pada jam sibuk, pelaksanaan uji beban (stress testing) secara berkala, serta penerapan sistem rekonsiliasi data transaksi otomatis berkecepatan tinggi dengan bank mitra, dilengkapi fitur live tracking status top-up pada aplikasi. Untuk risiko kelima yaitu Vulnerability API (Skor 5), strategi yang direkomendasikan adalah menerapkan arsitektur enkripsi end-to-end yang kuat pada setiap jalur API pihak ketiga, menetapkan standar autentikasi token yang ketat berbasis OAuth 2.0, serta melakukan audit keamanan melalui Penetration Testing secara berkala minimal satu kali per semester (Wijaya et al., 2025). Untuk risiko keenam yaitu Penyalahgunaan Paylater (Skor 9), strategi mitigasi meliputi penerapan verifikasi biometrik tambahan berupa pemindaian wajah (face recognition) atau PIN ganda sebelum pengguna menyetujui transaksi pemakaian limit kredit. Untuk risiko ketujuh yaitu Kegagalan KYC (Skor 6), rekomendasi mencakup integrasi teknologi OCR yang lebih akurat dan AI pendeteksi keaslian wajah (liveness detection) untuk mempercepat pencocokan data KTP secara real-time. Terakhir, untuk risiko kedelapan yaitu Insider Threat (Skor 5), penanganan dilakukan melalui penerapan prinsip Least Privilege yang membatasi hak akses karyawan hanya pada data yang diperlukan untuk tugasnya, pengaktifan logging aktivitas data yang ketat dan realtime, serta kewajiban penandatanganan Perjanjian Non-Pengungkapan (NDA) secara berkala bagi seluruh tim internal dan vendor mitra (Rofi, 2022).

KESIMPULAN

Penelitian ini berhasil memetakan delapan risiko keamanan utama pada ekosistem aplikasi DANA yang berdampak pada tiga pilar keamanan informasi yaitu confidentiality, integrity, dan availability. Melalui penerapan kerangka manajemen risiko ISO 31000:2018 yang diperkuat perspektif tata kelola IT dari COBIT 2019, evaluasi kuantitatif menghasilkan temuan bahwa serangan social engineering dan

phishing merupakan ancaman dengan prioritas tertinggi (skor 20), disusul penyalahgunaan akun via malware/APK palsu (skor 16). Kedua risiko ini dikategorikan Tinggi (High Risk) karena memiliki kombinasi frekuensi keterjadian yang sangat padat dengan dampak finansial yang seketika dan langsung dirasakan pengguna (Putri et al., 2021; Syadzwah et al., 2024). Enam risiko lainnya, termasuk Vulnerability API dan Insider Threat, berada dalam kategori Sedang (Medium Risk) dengan skor 5-9. Meskipun frekuensinya sangat jarang, bobot dampak yang sangat besar mengharuskan manajemen DANA untuk tidak mengabaikan sistem enkripsi dan kontrol hak akses harian. Temuan ini sejalan dengan hasil penelitian Uskono et al. (2025) yang menegaskan bahwa risiko teknis pada aplikasi fintech Indonesia memiliki karakteristik low frequency-high impact yang harus tetap menjadi perhatian utama tata kelola IT. Secara keseluruhan, strategi mitigasi yang direkomendasikan secara dominan berfokus pada penguatan fitur keamanan in-app berbasis kecerdasan buatan, otomatisasi infrastruktur cloud, penetration testing berkala, dan pengetatan hak akses berbasis prinsip least privilege, sejalan dengan rekomendasi domain APO12 dan EDM03 dalam kerangka COBIT 2019 (Syadzwah et al., 2024).

DAFTAR PUSTAKA

Nurrahma, D. A., Tanjung, N. N. Q., Gemilang, G. S., & Nurbaiti. (2025). Persepsi konsumen tentang keamanan data pada aplikasi ewallet: Studi kasus DANA. Jurnal Manuhara: Pusat Penelitian Ilmu Manajemen dan Bisnis, 3(3), 111-119.

Prastiwi, Y., Varel, E. Y., & Nainggolan, H. (2024). Analisis keamanan data pribadi dalam aplikasi mobile "DANA". Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB) 2024, 1–8.

Putri, M. Z., Sutarso, Y., & Hiqmah, F. (2021). Pengaruh risiko keamanan, keuangan dan sosial terhadap kepercayaan pada layanan mobile payment aplikasi dana. Journal Business and Banking, 11(1), 167-182.

Rofi, A. (2022). Manajemen risiko keamanan informasi pada organisasi. Jurnal Ilmiah Teknologi Informasi, 10(1), 45–58.

Salsabila, Z., Paramita, N. H., & Adtzimar, G. R. (2023). Pengaruh kemudahan, keamanan dan kepuasan pengguna terhadap penggunaan aplikasi dana. Indonesian Economics, Journal of Management and Accounting, 1(5), 335–339.

Savitri, E. (2021). Analisis risiko teknologi informasi menggunakan standar ISO 31000. Jurnal Sistem Informasi, 7(2), 112–124.

Syadzwah, D., Farensyah, I. E., dkk. (2024). Analisis kelemahan sistem aplikasi DANA dengan kerangka kerja COBIT 5.0 Domain DSS. Jurnal Teknologi Informasi dan Sistem Informasi Kelautan, 2(1), 34–42.

Tarigan, I. F. (2025). Analisis pola tren transaksi mencurigakan pada aplikasi DANA sebagai indikator fraud digital tahun 2020–2024. Jurnal Sistem Informasi, Akuntansi dan Manajemen, 5(2).

Umiyati, I., Putri, T. E., & Maya, N. (2021). Social influence, usability and security on the intensity of DANA ewallet use. Journal of Accounting for Sustainable Society (JASS), 3(1), 113–130.

Uskono, B. M., Wijaya, R., Pradipta, M. G., & Kusnadi, A. (2025). Analisis keamanan aplikasi fintech di Indonesia: Studi kasus OVO, GoPay, ShopeePay dan Dana. Journal of Informatic and Information Security, 5(2), 177–186.

Utomo, B. C., & Rahman, A. A. (2024). Analisis kesadaran keamanan data pribadi pada pengguna e-wallet DANA. Jurnal Riset Sains dan Teknologi, 8(1), 77–85.

Wijaya, A., Pandriadi, P., & Dini, M. (2025). Pengaruh efektivitas layanan dan transaction security terhadap penggunaan aplikasi DANA. Jurnal Akuntansi, Auditing dan Investasi, 5(1), 36–43.